# WELCOME TO NATO

This training program has been developed to help you learn the basics of working with NATO material. Each module consists of informational slides followed by one to five short quiz questions. As you complete each module you will be prompted to continue or quit. If you quit you can return to the next or previous module simply by choosing that button from the overview slide. At the end of the course you will be offered a ten question end of course test on which you must achieve a minimum of 60% to received a passing certificate.

We have attempted to simplify training by using this program but sometimes miss or overlook important information. Please forward comments, concerns, and questions to USAFE/SFXI.

NATO-Look Version 1.0/15 Aug 02/scl
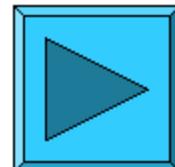
Course Modules

Select "Introduction" to begin.

INTRODUCTION TO NATO	**NATO IN U.S. DOCUMENTS**
CLASSIFICATIONS AND MARKINGS	**SAFEGUARDING**
ACCESS AUTHORIZATION	**ESPIONAGE**
THE REGISTRY SYSTEM	**END OF COURSE TEST**
ACCOUNTING FOR CLASSIFIED	**WHERE TO GO FOR HELP**

Introduction to NATO

The term **NATO** stands for:

North **A**tlantic **T**reaty **O**rganization

Introduction to NATO

NATO is made up of 19 nations who agree to comply with rules developed and approved by members

Belgium

Canada

Denmark

France

Germany

Poland

Greece

Iceland

Turkey

United States Of America

Italy

Portuga

Hungary

Spain

Norway

Czech Republic

United Kingdom

Netherlands

Luxembourg

Introduction to NATO

The

Secretary of Defense

Is the

United States

NATIONAL SECURITY AUTHORITY

For

NATO

Introduction to NATO

The Secretary of Defense is responsible for:

Ensuring that NATO security requirements are implemented throughout the Executive Branch of the United States Government

Introduction to NATO

What is NATO Information?
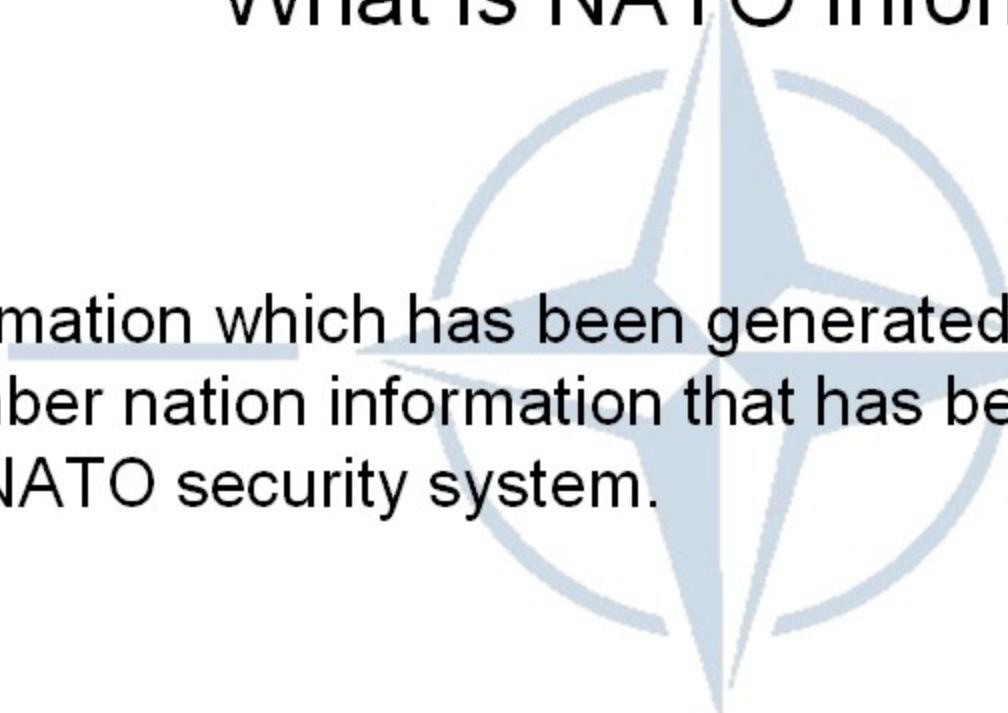
Information which has been generated by or for NATO, or member nation information that has been released into the NATO security system.

Introduction to NATO
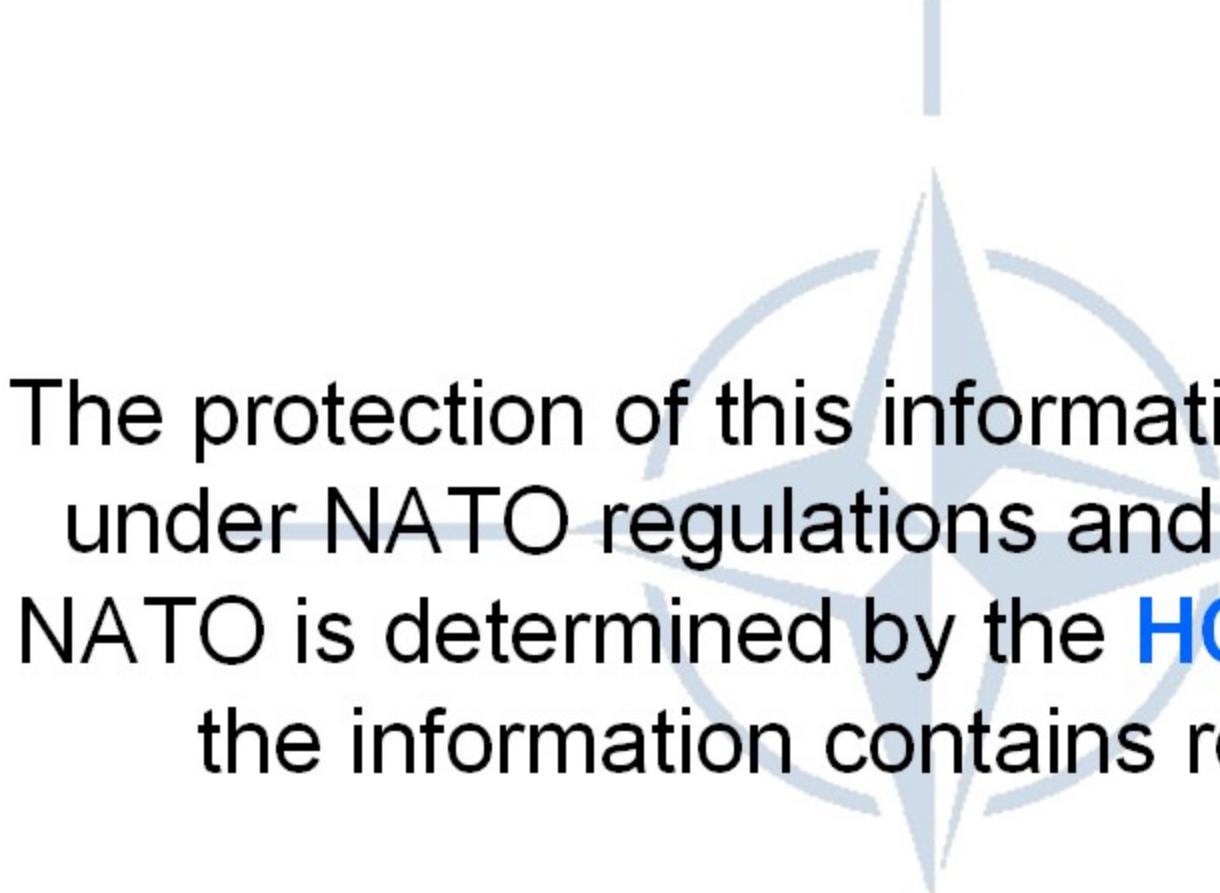
The protection of this information is controlled under NATO regulations and access within NATO is determined by the **HOLDER**, unless the information contains restrictions.

Introduction to NATO

Material may be generated by NATO or by a member nation.

If marked "NATO" by a member nation it is assumed to have been released to NATO.

However

Introduction to NATO

If the information has a national marking but is not marked "NATO" you SHOULD NOT apply NATO markings unless informed by the originator that the information may be released to NATO.

SO

Introduction to NATO
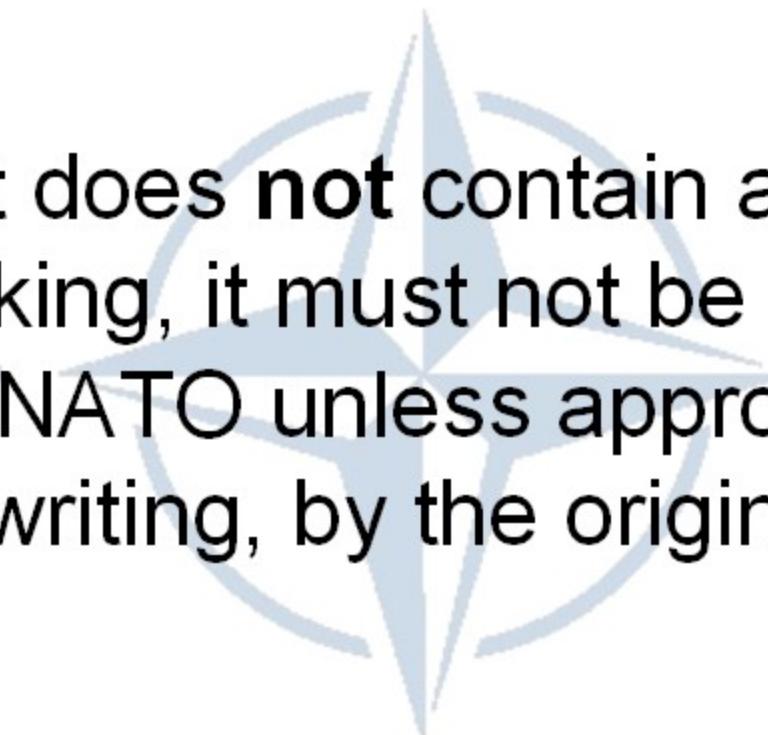
If it does **not** contain a NATO marking, it must not be released to NATO unless approved, in writing, by the originator.

Introduction to NATO

What about U.S material?

If the material can be released to NATO it will be marked with "RELEASABLE TO NATO"

Introduction to NATO
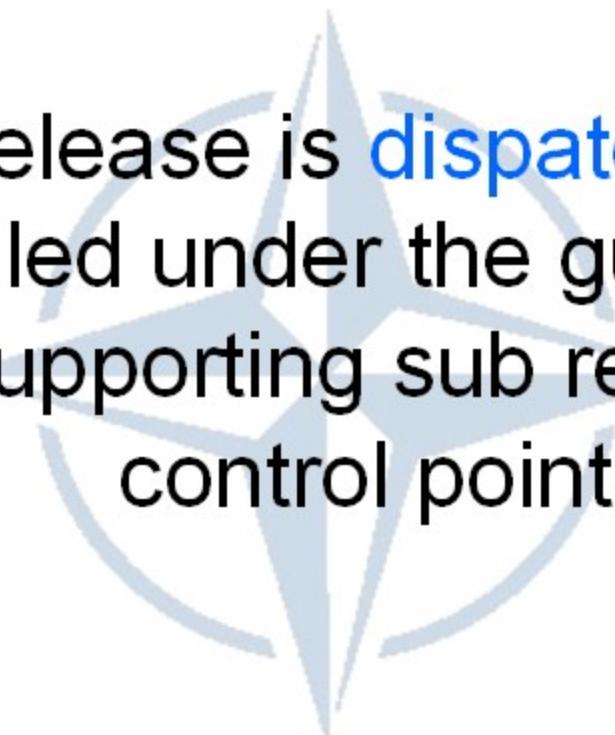
The release is dispatched and controlled under the guidance of the supporting sub registry or control point.

Introduction to NATO

If the material can be released to NATO it will be marked with "RELEASABLE TO NATO"

And will be controlled by the registry system

Markings and Categories

Four levels of classification

COSMIC TOP SECRET
NATO SECRET
NATO CONFIDENTIAL
NATO RESTRICTED

Markings and Categories

COSMIC TOP SECRET (CTS)

Unauthorized disclosure would cause exceptionally grave damage to NATO

The marking "COSMIC" is applied to TOP SECRET material to signify it is the property of NATO. **The term "NATO TOP SECRET" is not used.**

Markings and Categories

NATO SECRET (NS)

If unauthorized disclosure occurs would cause serious damage to NATO

Markings and Categories

NATO CONFIDENTIAL (NC)

An unauthorized disclosure would cause damage to the interests of NATO

Markings and Categories

NATO RESTRICTED (NR)

An unauthorized disclosure would be disadvantageous to the interests of NATO.

This is similar to FOR OFFICIAL USE ONLY, OFFICIAL USE ONLY, OR SENSITIVE, BUT UNCLASSIFIED information, **however NATO RESTRICTED is a security classification**.;

Markings and Categories

ATOMAL

Is either U.S Restricted Data or Formerly Restricted Data that is classified by the Atomic Energy Act of 1954.

It can be marked either COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA)

Classification Markings and Categories

NATO UNCLASSIFIED (NU)
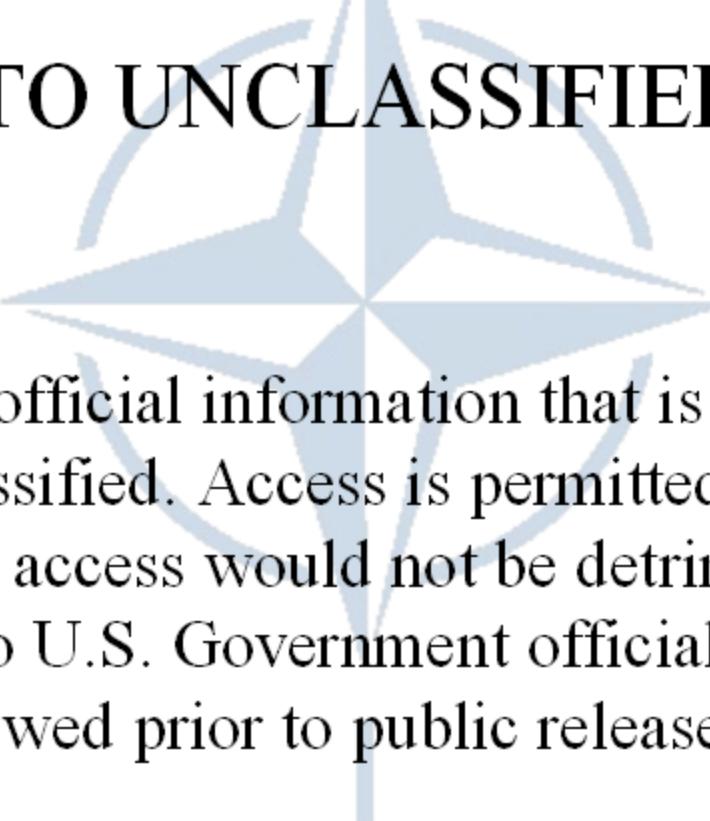
Is applied to official information that is NATO property but is not classified. Access is permitted by non-NATO entities when access would not be detrimental to NATO. It is similar to U.S. Government official information that must be reviewed prior to public release.

ACCESS AUTHORIZATION
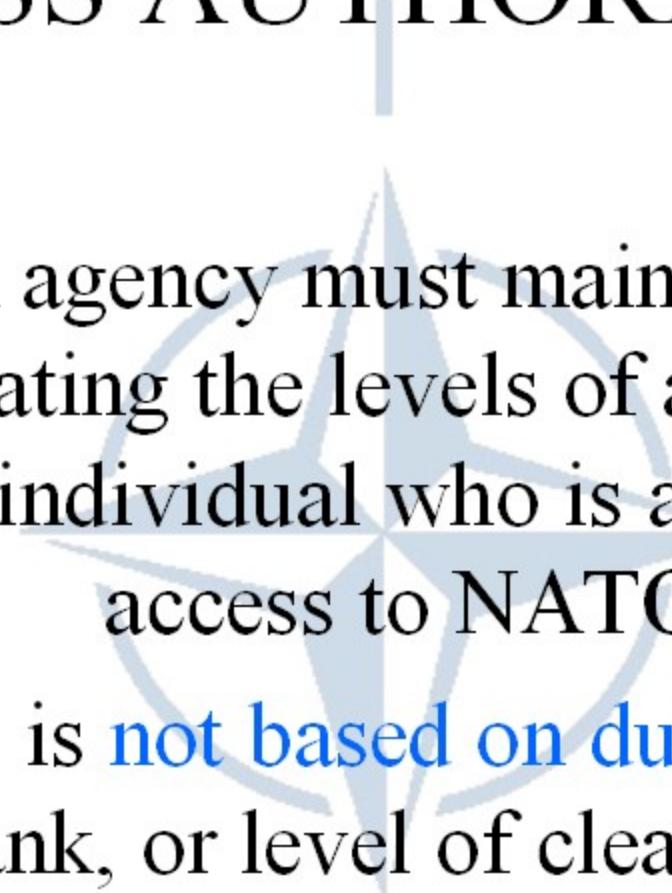
Each agency must maintain a list indicating the levels of access for each individual who is authorized access to NATO.

Access is not based on duty position, rank, or level of clearance.

ACCESS AUTHORIZATION
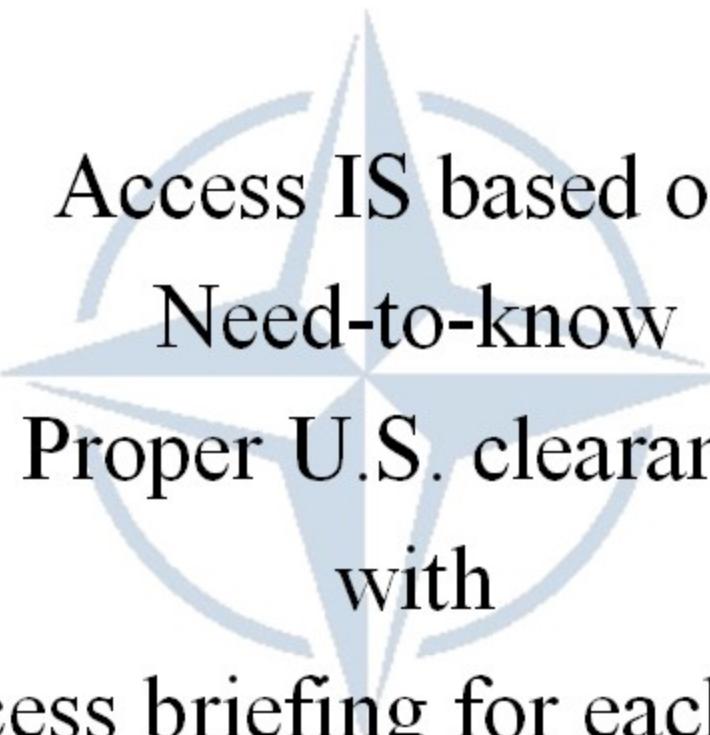
Access IS based on:

Need-to-know

Proper U.S. clearance

with

Access briefing for each level.

ACCESS AUTHORIZATION

Before you provide access it is
YOUR responsibility to ensure that
an individual is authorized.

If in doubt

Contact your Security Manager,
NATO sub registry or control point.

ACCESS AUTHORIZATION
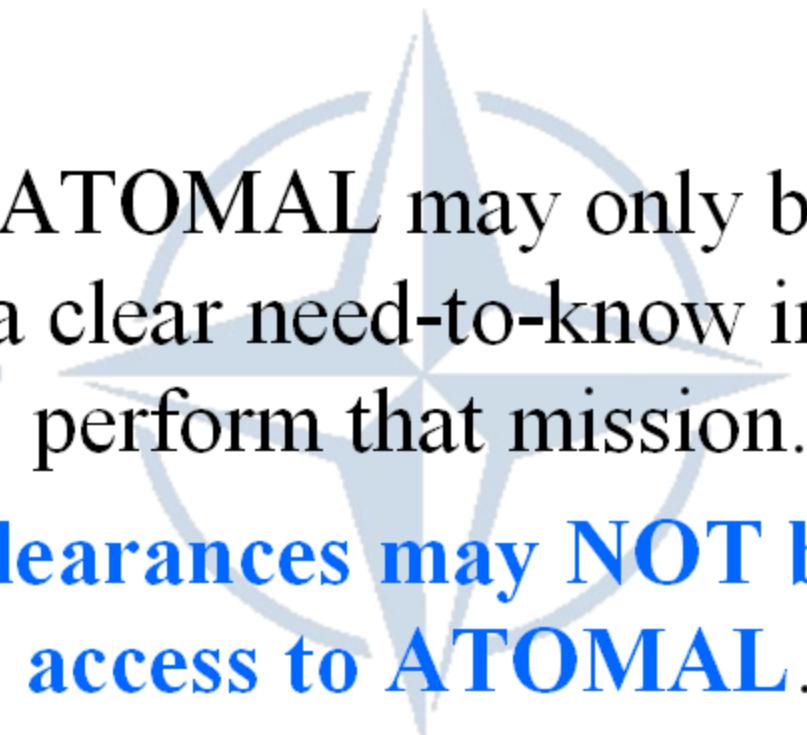
Access to ATOMAL may only be granted if there is a clear need-to-know in order to perform that mission.

Interim clearances may NOT be used for access to ATOMAL.

THE REGISTRY SYSTEM
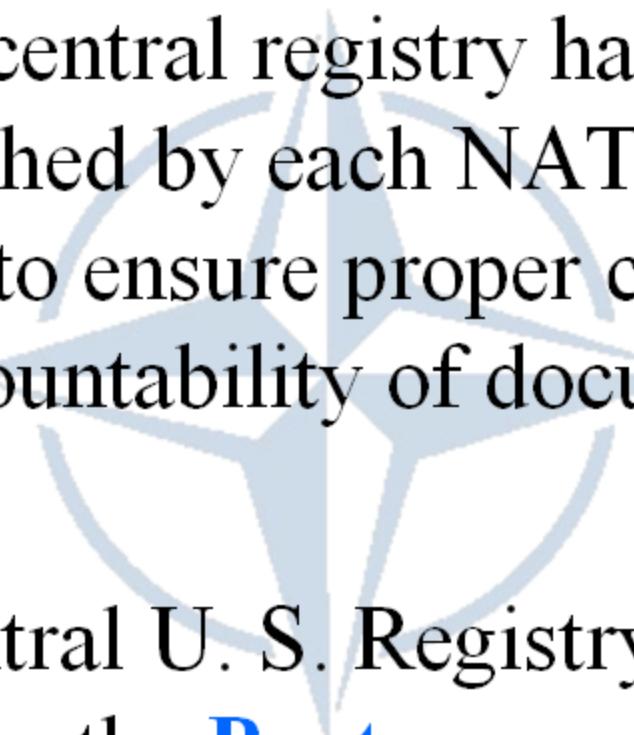
A central registry has been established by each NATO member nation to ensure proper control and accountability of documents.

The Central U. S. Registry (CUSR) is located in the **Pentagon** and oversees the administration of the U.S. registry system

THE REGISTRY SYSTEM
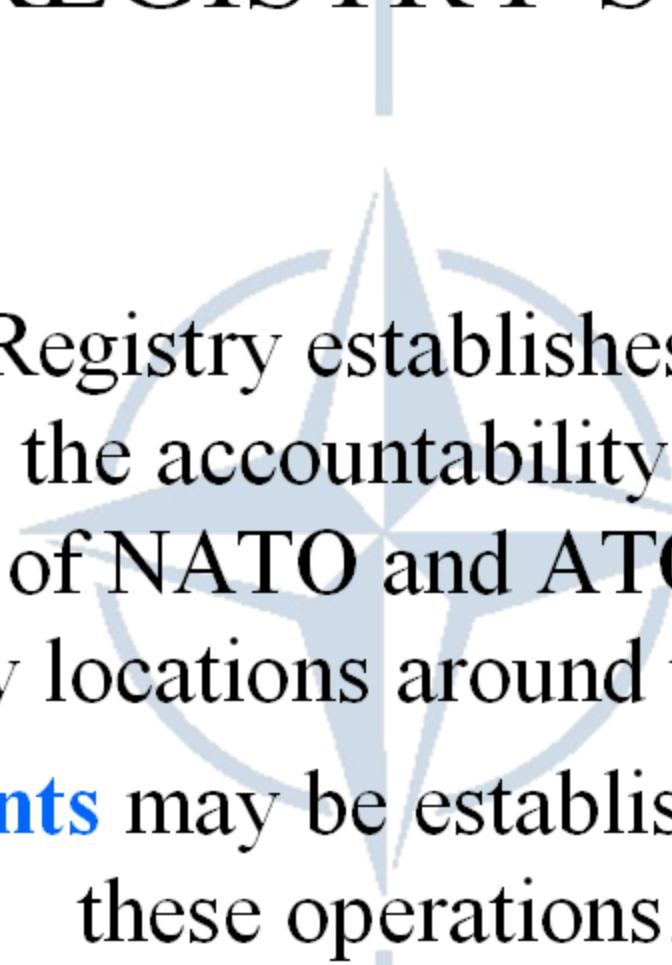
The Central Registry establishes **sub-registries** to execute the accountability and security management of NATO and ATOMAL material in many locations around the world. **Control points** may be established to assist in these operations.

ACCOUNTING FOR NATO MATERIAL

Receipts and logs must be maintained on the receipt, disposition, destruction, and dispatch of **COSMIC**, **NATO SECRET**, and all **ATOMAL** material.

ACCOUNTING FOR NATO MATERIAL

Individuals must execute a disclosure record upon acquiring access to each item of CTS/CTSA material.

ACCOUNTING FOR NATO MATERIAL
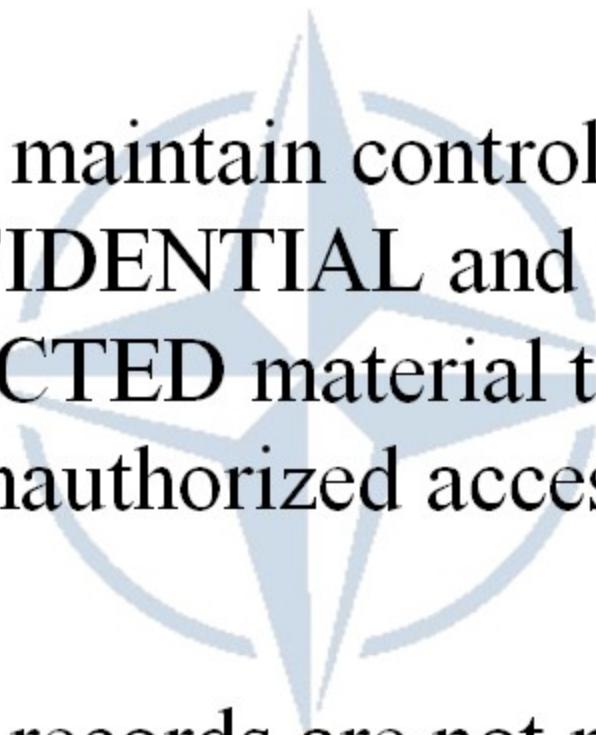
You must maintain control of NATO CONFIDENTIAL and NATO RESTRICTED material to prevent unauthorized access.

Specific records are not necessary unless required by the originator.

MARKING AND ACCOUNTING FOR U.S. DOCUMENTS CONTAINING NATO

Instructions must indicate that the information can not be downgraded or declassified without prior consent of NATO

Cite: "foreign government information"

SAFEGUARDING
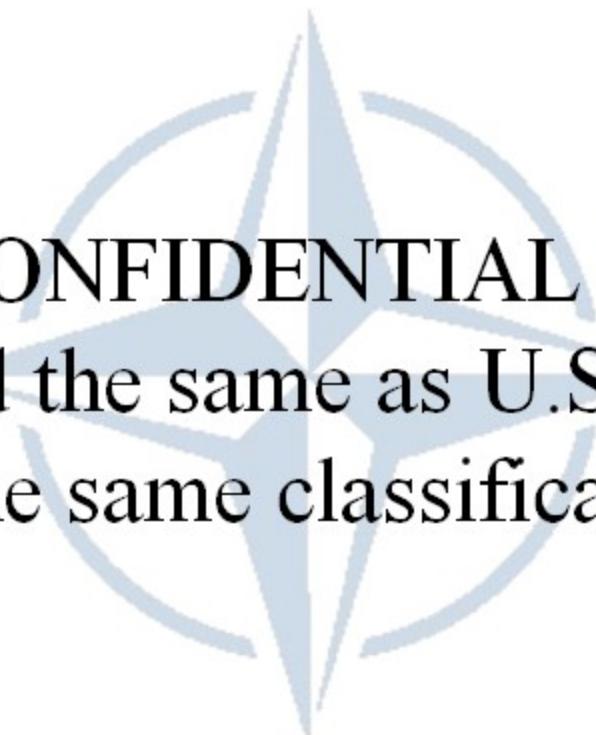
NATO CONFIDENTIAL and above are stored the same as U.S. material of the same classification.

SAFEGUARDING

NATO RESTRICTED may be stored in a **locked filing cabinet**, or in a **room or building that is locked** during non-duty hours as long as access to the material can only be gained by authorized personnel.

SAFEGUARDING
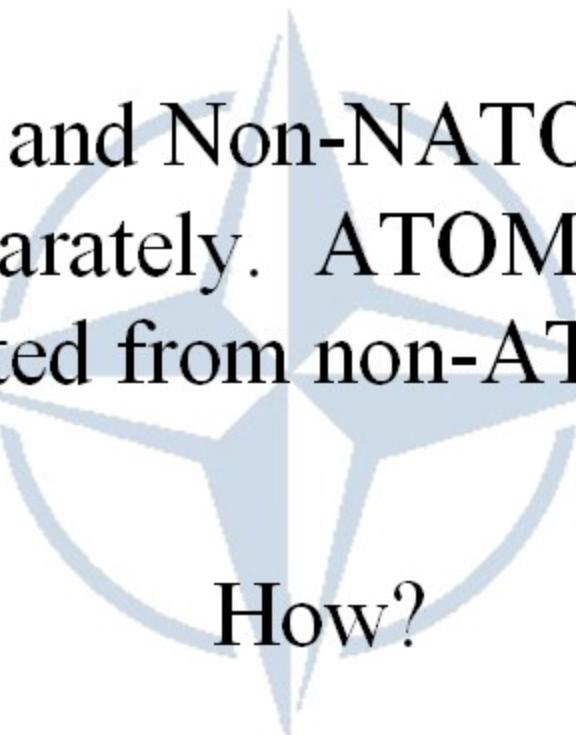
NATO and Non-NATO must be stored separately. ATOMAL must be separated from non-ATOMAL.

How?

SAFEGUARDING
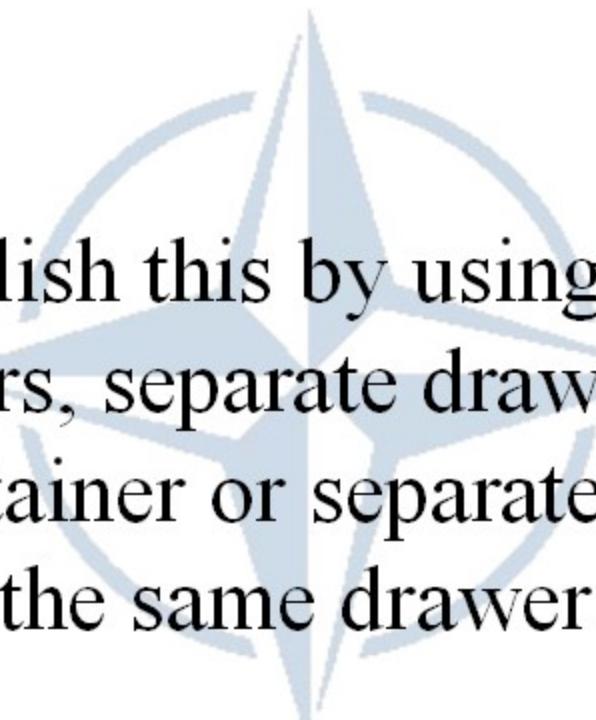
Accomplish this by using separate containers, separate drawers in the same container or separate folders in the same drawer.

SAFEGUARDING
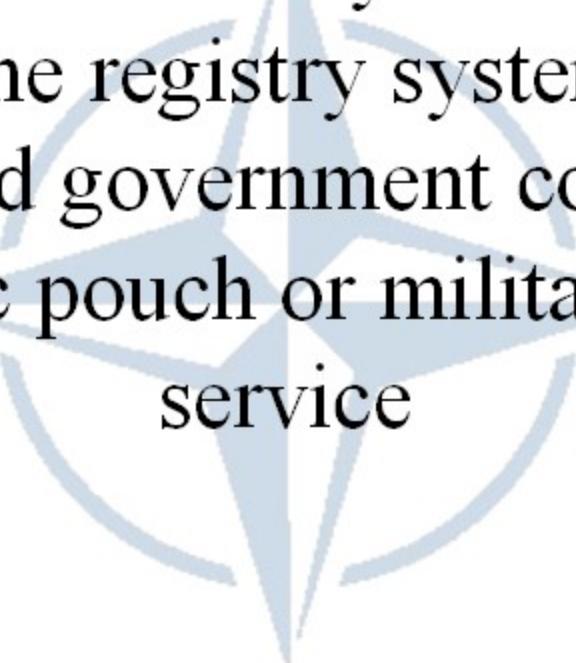
CTS/CTSA can only be transported through the registry system using a cleared government courier, diplomatic pouch or military courier service

SAFEGUARDING

All other NATO must be by cleared courier or by cleared and briefed employees who possess courier identification and authorization or by U.S Registered mail using same rules as U.S. classified

Receipt is required for all ATOMAL and NS material

SAFEGUARDING

Automated Information Systems (AIS)

Same security standards as U.S. classified except organizations must issue instructions for processing, handing and accounting for NATO information.

SAFEGUARDING

Destruction of CTS, CTSA, NS, NSA, NCA

May only be accomplished by registry system personnel using a certificate and method approved for the destruction of U.S. material of the same classification.

SAFEGUARDING

Destruction

[NR/NC]
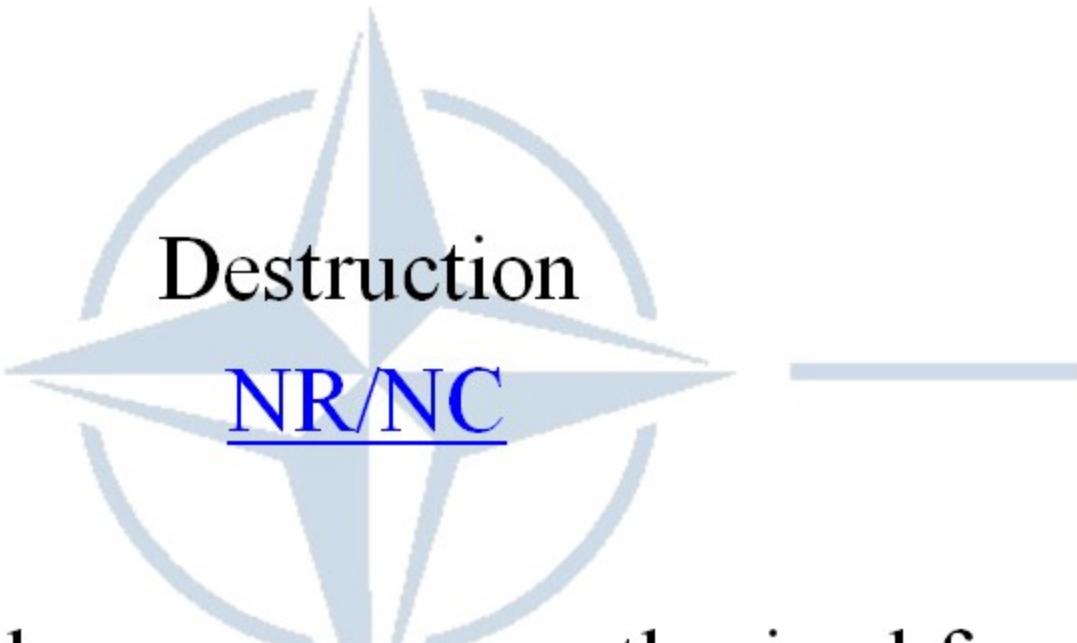
Destroy by any means authorized for U.S. CONFIDENTIAL.

SAFEGUARDING

Reproduction

COSMIC can only be reproduced by the CUSR and COSMIC Sub registries

Number of copies must be reported to CUSR.

SAFEGUARDING

ATOMAL may be copied [CUSR](), Sub registries, and ATOMAL Control Points

SAFEGUARDING

NS and below may reproduced by the holder of the information with strict need-know. Copies are accounted for, marked, and safeguarded in the same manner as the original
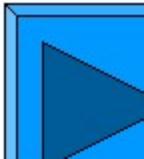
SECURITY VIOLATIONS
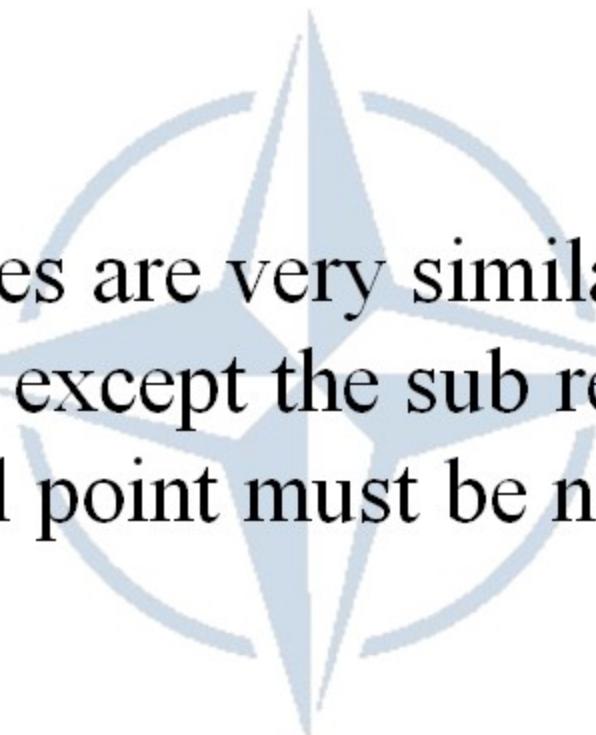
Guidelines are very similar to U.S. Material except the sub registry or control point must be notified.

ESPIONAGE, SABOTAGE, TERRORISM

STAY CALM: You are not at fault because they chose to target you.
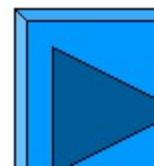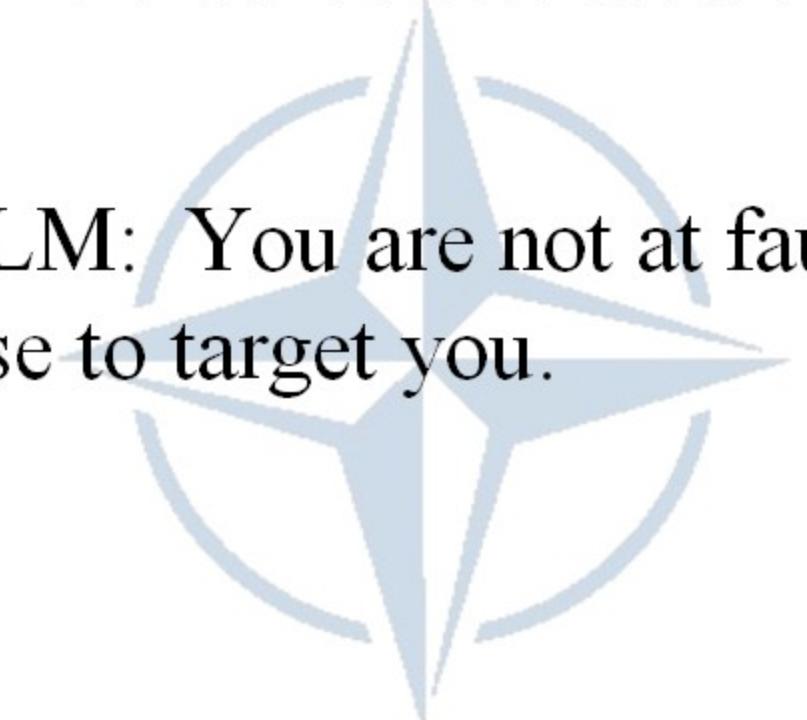
ESPIONAGE, SABOTAGE, TERRORISM

BE NONCOMMITTAL: Be ambiguous as to whether or not you will provide them with material or information.

ESPIONAGE, SABOTAGE, TERRORISM

REPORT IT PROMPTLY: Even if it seems purely coincidental or insignificant, a small detail may be the key to an attempt. Do not discuss the incident with friends, family, co-workers, etc., unless directed to by a security officer.